



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/532,072	01/09/2006	Takeshi Tanaka	1.8638.05102	4037
52989	7590	03/24/2010		
Dickinson Wright PLLC James E. Ledbetter, Esq. International Square 1875 Eye Street, N.W., Suite 1200 Washington, DC 20006			EXAMINER PHAM, TIMOTHY X	
			ART UNIT 2617	PAPER NUMBER
			MAIL DATE 03/24/2010	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

### Office Action Summary

**Application No.**

10/532,072

**Applicant(s)**

TANAKA ET AL.

**Examiner**

TIMOTHY PHAM

**Art Unit**

2617

**Period for Reply** -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 14 January 2010.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1,2,4,5,9,10,12-14,16,17,19,20,40,41 and 43-54 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-2,4-5,9-10,12-14,16-17,19-20,40-41,43-54 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-940)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

## DETAILED ACTION

### *Response to Arguments*

1. Applicant's arguments filed 1/14/2010 have been fully considered but they are not persuasive.

On page 15, 2<sup>nd</sup> paragraph, of the Applicant's Response, applicant argues that "*The Office Action provides no findings of fact to support an inference that Inoue discloses the Applicants' claimed subject matter of setting a time for acquiring an authentication result*", with the corresponding teaching indicating the arguments and the arts references below, the Examiner respectfully disagrees. Inoue discloses setting a time until acquiring the authentication result (paragraphs [0017], [0023], [0028], [0067], [0133]). During patent examination, the claims must be given their broadly reasonable interpretation. See MPEP 2111. The term "setting a time until acquiring the authentication result" is broadly claimed, therefore, it is broadly interpreted.

The Examiner respectfully disagrees with Applicant's arguments because Saito in combination with Malki and Inoue as a whole, teaches what claim 1 recites – that is Malki discloses setting a predetermined tentative permission time for which the mobile terminal tentatively permits an access to the desired network (paragraph [0055], e.g., the lifetime of the bicasting should be set to no more than 10 seconds to limit the load imposed on the network by the bicasting) and Inoue discloses setting a time until acquiring the authentication result (paragraphs [0017], [0023], [0028], [0067], [0133], e.g., it is possible to enable the authenticated telephone network access by defining the authentication sequence between the home network device and the mobile terminal device, and the access to the resource on the cellular phone

network side is permitted only for the device that has successfully completed the authentication sequence).

MPEP 2144 states that the strongest rationale for combining references is a recognition, expressly or impliedly in the prior art or drawn from a convincing line of reasoning based on established scientific principles or legal precedent, that some advantage or expected beneficial result would have been produced by their combination. *In re Sernaker*, 702 F.2d 989, 994-95, 217 USPQ 1, 5-6 (Fed. Cir. 1983). See also *Dystar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick*, 464 F.3d 1356, 1368, 80 USPQ2d 1641, 1651 (Fed. Cir. 2006). As stated in the last Office Action, , it would have been obvious to one having ordinary skill in the art at the time of the invention by applicant to set a time until acquiring the authentication result for advantages of providing a communication system in which a mobile terminal device belonging to some mobile carrier network can access a fixed communication network via a local network/gateway even when this mobile terminal device does not have a right or a qualification for accessing the fixed communication network via the local network/gateway that is given in advance (Inoue: paragraph [0014]).

### ***Claim Rejections - 35 USC § 103***

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-2, 4-5, 10, 12-13,4, 17, 19-20, 40-41, 43-45, 47-50, 53-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Saito (US 2002/0172207; Cited in IDS) in view of

Malki et al. (hereinafter "Malki"; US 2001/0046223; same as WO 01067798 cited in IDS) and Inoue (US 2002/0036991; Cited in PTO-892 Part of Paper 20091008).

Regarding claim 1, Saito discloses a radio communication management method in a radio communication system which manages link connection of a mobile terminal using HMIPv6 (paragraphs [0008], [0030], [0178], noted an IPv6),

wherein the mobile terminal transmits information on authentication for accessing a desired network together with first information for changing the link connection with respect to a server which manages the link connection of the mobile terminal to reduce a time required for changing the link connection of the mobile terminal (Fig. 30, references S104 through S108; paragraphs [0010], [0015], [0019], [0022]-[0023], [0028], [0030], where Saito discusses the operation configuration for reporting a location change including authentication data each time a terminal moves between subnets, and achieves scalability an handoff by driving a network area into two layers using two different protocols),

wherein the server (Fig. 7, reference 304) which manages the link connection acquires an authentication result by an authentication process using the information on the authentication (Fig. 6; paragraphs [0016], [0019], [0023]-[0024], [0269], [0355], e.g., the terminal device 302 determines whether authentication data stored in the binding update packet is valid or not, and if it is valid, then registers the care-of-address of the terminal 301), and

wherein the server which manages the link connection, after receiving the first information, transmits, to the mobile terminal, information notifying the permission of the access to the desired network only for the predetermined tentative permission time together with the information notifying that the change of the link connection of the mobile terminal has been

confirmed (paragraph [0052], e.g., the gateway router performs a duplication check for the current address of the mobile node, and transmits a registration acknowledgement message including the check result to the mobile node), and

then the server which manages the link connection transmits the authentication result to the mobile terminal together with information notifying that the change of the link connection of the mobile terminal has been confirmed, when next receiving second information for changing the link connection from the mobile terminal in a case where the authentication result is capable of being acquired within the time until acquiring the authentication result (paragraphs [0052], [0079], [0089], [0109], e.g., when the duplication check result for a current address of the mobile node is affirmative).

Saito fails to specifically disclose setting a predetermined tentative permission time for which the mobile terminal tentatively permits an access to the desired network and setting a time until acquiring the authentication result.

However, Malki discloses setting a predetermined tentative permission time for which the mobile terminal tentatively permits an access to the desired network (paragraph [0055], e.g., the lifetime of the bicasting should be set to no more than 10 seconds to limit the load imposed on the network by the bicasting).

Therefore, taking teachings of Saito in combination of Malki as a whole, it would have been obvious to one having ordinary skill in the art at the time of the invention by applicant to set a predetermined permission time to permit the mobile terminal to access to the desired network while the authentication process is processing for advantages of improving communication processing for a mobile communication device.

Saito in combination with Malki fails to disclose setting a time until acquiring the authentication result.

However, Inoue discloses setting a time until acquiring the authentication result (paragraphs [0017], [0023], [0028], [0067], [0133], e.g., it is possible to enable the authenticated telephone network access by defining the authentication sequence between the home network device and the mobile terminal device, and the access to the resource on the cellular phone network side is permitted only for the device that has successfully completed the authentication sequence).

Therefore, taking teachings of Saito in combination of Malki and Inoue as a whole, it would have been obvious to one having ordinary skill in the art at the time of the invention by applicant to set a time until acquiring the authentication result for advantages of providing a communication system in which a mobile terminal device belonging to some mobile carrier network can access a fixed communication network via a local network/gateway even when this mobile terminal device does not have a right or a qualification for accessing the fixed communication network via the local network/gateway that is given in advance (Inoue: paragraph [0014]).

Regarding claim 2, Saito in combination with Malki and Inoue discloses the radio communication management method according to claim 1 above, wherein the mobile terminal transmits the first information for changing the link connection and the information on the authentication as one piece of (Saito: paragraph [0010], e.g., The terminal device (mobile node) 301 generates a binding update packet including a home address, care-of-address, and authentication data for the terminal device 301, and transmits the packet to a home agent 302),

and the server which manages the link connection acquires each of the first information for changing the link connection and the information on the authentication from the one piece of information (Saito: Abstract; paragraphs [0027], [0030], [0048], [0050], [0180]-[0181], [0326], e.g., a mobile node periodically transmits movement information of the node or transmit information when moving between sub-networks to a home agent).

Regarding claim 4, Saito in combination with Malki and Inoue discloses the radio communication management method according to claim 1 above, wherein the server which manages the link connection communicates with an authentication server which authenticates the mobile terminal to acquire the authentication result (Saito: Fig. 7; paragraphs [0016], [0019], [0023]-[0024], e.g., the home agent 302 check whether the authentication data is valid or not, and if it determines that the data is valid, it registers the care-of-address).

Regarding claim 5, Saito in combination with Malki and Inoue discloses the radio communication management method according to claim 1 above, comprising the step of: transmitting the information notifying that the change of the link connection of the mobile terminal has been confirmed (Saito: paragraph [0019], e.g., the terminal device 303 checks the authentication data, and if it determines that the data is valid, it registers the care-of-address of the terminal device 301 in the binding cache) and the authentication result as one piece of information to the mobile terminal (Saito: paragraphs [0023]-[0024], e.g., the home agent 302 determines whether authentication data stored in the binding update packet is valid or not).

Regarding claim 10, Saito in combination with Malki and Inoue discloses the radio communication management method according to claim 1 above, wherein the server which manages the link connection performs registration relating to the change of the link connection



of the mobile terminal which has permitted the access to the desired network for the predetermined tentative permission time or only for a the predetermined permission time (Saito: paragraphs [0054], e.g., the gateway router set a lifetime of the routing cache for each mobile node in accordance with a routing update interval time), and deletes the registration relating to the change of the link connection of the mobile terminal in a case where the predetermined tentative permission time or the predetermined permission time has elapsed (Saito: paragraphs [0272], [0295], e.g., the gateway router transmits the registration acknowledgement message to the access router to advertise that the registration is not permitted because the address is duplicated, then the paging cache is deleted after a predetermine time).

Regarding claim 12, Saito in combination with Malki and Inoue discloses the radio communication management method according to claim 5 above, wherein the server which manages the link connection sets a predetermined connection prohibition time with respect to the mobile terminal (Saito: paragraphs [0054], e.g., the gateway router set a lifetime of the routing cache for each mobile node in accordance with a routing update interval time), and does not perform a process relating to the change of the link connection of the mobile terminal which has failed in the authentication and a process relating to the authentication for the predetermined connection prohibition time after notification of authentication failure in a case where the authentication failure is notified as the authentication result with respect to the mobile terminal (Inoue: paragraph [0127], e.g., when the authentication fails, i.e., when the two message authentication codes do not coincide in the above example (step S12 NO), Nack message is returned to the device (step S15) and the subsequent access from the device 2 will not be transferred to the cellular phone network 6).

Therefore, taking teachings of Saito in combination of Malki and Inoue as a whole, it would have been obvious to one having ordinary skill in the art at the time of the invention by applicant by not performing a process relating to the change of the link connection of the mobile terminal which has failed in the authentication and a process relating to the authentication for the predetermined connection prohibition time after notification of authentication failure in a case where the authentication failure is notified as the authentication result with respect to the mobile terminal for advantages of providing a communication system in which a mobile terminal device belonging to some mobile carrier network can access a fixed communication network via a local network/gateway even when this mobile terminal device does not have a right or a qualification for accessing the fixed communication network via the local network/gateway that is given in advance (Inoue: paragraph [0014]).

Regarding claim 13, Saito in combination with Malki and Inoue discloses the radio communication management method according to claim 5 above, wherein the server which manages the link connection performs registration relating to the change of the link connection of the mobile terminal which has succeeded in the authentication only in a case where authentication success is notified as the authentication result with respect to the mobile terminal (Inoue: paragraph [0126], e.g., When the authentication succeeds, i.e., when the two message authentication codes coincide in the above example (step S12 YES), Ack message is returned to the device 2 and the subsequent access from the device 2 will be transferred to the cellular phone network 6 (step S13) ).

Therefore, taking teachings of Saito in combination of Malki and Inoue as a whole, it would have been obvious to one having ordinary skill in the art at the time of the invention by

applicant to perform registration relating to the change of the link connection of the mobile terminal which has succeeded in the authentication only in a case where authentication success is notified as the authentication result with respect to the mobile terminal for advantages of providing a communication system in which a mobile terminal device belonging to some mobile carrier network can access a fixed communication network via a local network/gateway even when this mobile terminal device does not have a right or a qualification for accessing the fixed communication network via the local network/gateway that is given in advance (Inoue: paragraph [0014]).

Regarding claim 14, Saito discloses a radio communication management method in a radio communication system which manages link connection of a mobile terminal,

wherein the mobile terminal transmits information on authentication for accessing a desired network together with information for changing the link connection with respect to a server which manages the link connection of the mobile terminal (Fig. 30, references S104 through S108; paragraphs [0010], [0015], [0019], [0022]-[0023], [0028], [0030], where Saito discusses the operation configuration for reporting a location change including authentication data each time a terminal moves between subnets, and achieves scalability an handoff by driving a network area into two layers using two different protocols), and

the server (Fig. 7, reference 304) which managing the link connection, after receiving the information for changing the link connection, transmits, to the mobile terminal, information notifying the permission of the access to the desired network only for the predetermined tentative permission time confirmed (paragraph [0052], e.g., the gateway router performs a duplication

check for the current address of the mobile node, and transmits a registration acknowledgement message including the check result to the mobile node), and

the server which manages the link connection transmits the authentication result to the mobile terminal in a case where the authentication result is capable of being acquired within the time until acquiring the authentication result (paragraphs [0052], [0079], [0089], [0109], e.g., when the duplication check result for a current address of the mobile node is affirmative).

Saito fails to specifically disclose setting a predetermined tentative permission time for which the mobile terminal tentatively permits an access to the desired network and setting a time until acquiring the authentication result.

However, Malki discloses setting a predetermined tentative permission time for which the mobile terminal tentatively permits an access to the desired network (paragraph [0055], e.g., the lifetime of the bicasting should be set to no more than 10 seconds to limit the load imposed on the network by the bicasting).

Therefore, taking teachings of Saito in combination of Malki as a whole, it would have been obvious to one having ordinary skill in the art at the time of the invention by applicant to set a predetermined permission time to permit the mobile terminal to access to the desired network while the authentication process is processing for advantages of improving communication processing for a mobile communication device.

Saito in combination with Malki fails to disclose setting a time until acquiring the authentication result.

However, Inoue discloses setting a time until acquiring the authentication result (paragraphs [0017], [0023], [0028], [0067], [0133], e.g., it is possible to enable the authenticated

telephone network access by defining the authentication sequence between the home network device and the mobile terminal device, and the access to the resource on the cellular phone network side is permitted only for the device that has successfully completed the authentication sequence).

Therefore, taking teachings of Saito in combination of Malki and Inoue as a whole, it would have been obvious to one having ordinary skill in the art at the time of the invention by applicant to set a time until acquiring the authentication result for advantages of providing a communication system in which a mobile terminal device belonging to some mobile carrier network can access a fixed communication network via a local network/gateway even when this mobile terminal device does not have a right or a qualification for accessing the fixed communication network via the local network/gateway that is given in advance (Inoue: paragraph [0014]).

Regarding claim 17, Saito in combination with Malki and Inoue discloses the radio communication management method according to claim 14 above, wherein the server which manages the link connection cuts the connection of the mobile terminal in a case where the predetermined tentative permission time or a predetermined permission time has elapsed (Saito: paragraphs [0272], [0295], e.g., the gateway router transmits the registration acknowledgement message to the access router to advertise that the registration is not permitted because the address is duplicated, then the paging cache is deleted after a predetermine time).

Regarding claim 19, Saito in combination with Malki and Inoue discloses the radio communication management method according to claim 14 above, wherein the server which manages the link connection sets a predetermined connection prohibition time with respect to the

mobile terminal (Saito: paragraphs [0054], e.g., the gateway router set a lifetime of the routing cache for each mobile node in accordance with a routing update interval time), and does not perform a process relating to the mobile terminal which has failed in the authentication only for the predetermined connection prohibition time after notification of the authentication failure in a case where the authentication failure is notified as the authentication result with respect to the mobile terminal (Inoue: paragraph [0127], e.g., when the authentication fails, i.e., when the two message authentication codes do not coincide in the above example (step S12 NO), Nack message is returned to the device (step S15) and the subsequent access from the device 2 will not be transferred to the cellular phone network 6).

Therefore, taking teachings of Saito in combination of Malki and Inoue as a whole, it would have been obvious to one having ordinary skill in the art at the time of the invention by applicant by not performing a process relating to the change of the link connection of the mobile terminal which has failed in the authentication and a process relating to the authentication for the predetermined connection prohibition time after notification of authentication failure in a case where the authentication failure is notified as the authentication result with respect to the mobile terminal for advantages of providing a communication system in which a mobile terminal device belonging to some mobile carrier network can access a fixed communication network via a local network/gateway even when this mobile terminal device does not have a right or a qualification for accessing the fixed communication network via the local network/gateway that is given in advance (Inoue: paragraph [0014]).

Regarding claim 20, Saito in combination with Malki and Inoue discloses the radio communication management method according to claim 14 above, wherein the server which

manages the link connection performs registration relating to the change of the link connection of the mobile terminal which has succeeded in the authentication only in a case where authentication success is notified as the authentication result with respect to the mobile terminal (Inoue: paragraph [0126], e.g., When the authentication succeeds, i.e., when the two message authentication codes coincide in the above example (step S12 YES), Ack message is returned to the device 2 and the subsequent access from the device 2 will be transferred to the cellular phone network 6 (step S13) ).

Therefore, taking teachings of Saito in combination of Malki and Inoue as a whole, it would have been obvious to one having ordinary skill in the art at the time of the invention by applicant to perform registration relating to the change of the link connection of the mobile terminal which has succeeded in the authentication only in a case where authentication success is notified as the authentication result with respect to the mobile terminal for advantages of providing a communication system in which a mobile terminal device belonging to some mobile carrier network can access a fixed communication network via a local network/gateway even when this mobile terminal device does not have a right or a qualification for accessing the fixed communication network via the local network/gateway that is given in advance (Inoue: paragraph [0014]).

Claims 40-41 are rejected with the same reasons set forth to claims 12-13 respectively.

Regarding claim 43, Saito discloses a radio communication management server which manages link connection of a mobile terminal using HMIPv6 (paragraphs [0008], [0030], [0178], noted an IPv6), constituted to receive, from the mobile terminal, first information for changing the link connection and information on authentication for accessing a desired network as one

piece of information, and acquire each of the first information for changing the link connection and the information on the authentication from the one piece of information and to acquire an authentication result by an authentication process using the information on the authentication (Fig. 30, references S104 through S108; paragraphs [0010], [0015], [0019], [0022]- [0023], [0028], [0030], where Saito discusses the operation configuration for reporting a location change including authentication data each time a terminal moves between subnets, and achieves scalability an handoff by driving a network area into two layers using two different protocols), comprising:

the radio communication management server further constituted to, after receiving the first information, transmit, to the mobile terminal, information notifying the permission of the access to the desired network only for the predetermined tentative permission time together with the information notifying that the change of the link connection of the mobile terminal has been confirmed (paragraph [0052], e.g., the gateway router performs a duplication check for the current address of the mobile node, and transmits a registration acknowledgement message including the check result to the mobile node), and

then to transmit the authentication result to the mobile terminal together with information notifying that the change of the link connection of the mobile terminal has been confirmed, when next receiving second information for changing the link connection from the mobile terminal in a case where the authentication result is capable of being acquired within the time until acquiring the authentication result (paragraphs [0052], [0079], [0089], [0109], e.g., when the duplication check result for a current address of the mobile node is affirmative).



Saito fails to specifically disclose a first time setting section that sets a time until acquiring the authentication result, and a second time setting section that sets a predetermined tentative permission time to tentatively permit an access to the desired network with respect to the mobile terminal.

However, Malki discloses setting a predetermined tentative permission time for which the mobile terminal tentatively permits an access to the desired network with respect to the mobile terminal (paragraph [0055], e.g., the lifetime of the bicasting should be set to no more than 10 seconds to limit the load imposed on the network by the bicasting).

Therefore, taking teachings of Saito in combination of Malki as a whole, it would have been obvious to one having ordinary skill in the art at the time of the invention by applicant to set a predetermined permission time to permit the mobile terminal to access to the desired network while the authentication process is processing for advantages of improving communication processing for a mobile communication device.

Saito in combination with Malki fails to disclose setting a time until acquiring the authentication result.

However, Inoue discloses setting a time until acquiring the authentication result (paragraphs [0017], [0023], [0028], [0067], [0133], e.g., it is possible to enable the authenticated telephone network access by defining the authentication sequence between the home network device and the mobile terminal device, and the access to the resource on the cellular phone network side is permitted only for the device that has successfully completed the authentication sequence).

Therefore, taking teachings of Saito in combination of Malki and Inoue as a whole, it would have been obvious to one having ordinary skill in the art at the time of the invention by applicant to set a time until acquiring the authentication result for advantages of providing a communication system in which a mobile terminal device belonging to some mobile carrier network can access a fixed communication network via a local network/gateway even when this mobile terminal device does not have a right or a qualification for accessing the fixed communication network via the local network/gateway that is given in advance (Inoue: paragraph [0014]).

Regarding claim 44 Saito in combination with Malki and Inoue discloses the radio communication management server according to claim 43 above, further comprising a unit which communicates with an authentication server which authenticates the mobile terminal to acquire the authentication result (Saito: Fig. 7; paragraphs [0016], [0019], [0023]-[0024], e.g., the home agent 302 check whether the authentication data is valid or not, and if it determines that the data is valid, it registers the care-of-address).

Regarding claim 45 Saito in combination with Malki and Inoue discloses the radio communication management server according to claim 43 above, constituted to transmit, to the mobile terminal, the information notifying that the change of the link connection of the mobile terminal has been confirmed (Saito: paragraph [0019], e.g., the terminal device 303 checks the authentication data, and if it determines that the data is valid, it registers the care-of-address of the terminal device 301 in the binding cache) and the authentication result as one piece of information (Saito: paragraphs [0023]-[0024], e.g., the home agent 302 determines whether authentication data stored in the binding update packet is valid or not).

Regarding claim 47 Saito in combination with Malki and Inoue discloses the radio communication management server according to claim 43 above, further comprising:

an information registration unit which performs registration relating to the change of the link connection of the mobile terminal which has permitted the access to the desired network for the predetermined tentative permission time or only for a predetermined permission time (Saito: paragraphs [0054], e.g., the gateway router set a lifetime of the routing cache for each mobile node in accordance with a routing update interval time); and

an information deletion unit which deletes the registration relating to the change of the link connection of the mobile terminal in a case where the predetermined tentative permission time or the predetermined permission time has elapsed (Saito: paragraphs [0272], [0295], e.g., the gateway router transmits the registration acknowledgement message to the access router to advertise that the registration is not permitted because the address is duplicated, then the paging cache is deleted after a predetermine time).

Regarding claim 48 Saito in combination with Malki and Inoue discloses the radio communication management server according to claim 43 above, further comprising:

a prohibition time setting unit which sets a predetermined connection prohibition time with respect to the mobile terminal (Saito: paragraphs [0054], e.g., the gateway router set a lifetime of the routing cache for each mobile node in accordance with a routing update interval time); and

a prohibition control unit which controls to prevent a process relating to the change of the link connection of the mobile terminal which has failed in the authentication and a process relating to the authentication from being performed for the predetermined connection prohibition

time after notification of authentication failure in a case where the authentication failure is notified as the authentication result with respect to the mobile terminal (Inoue: paragraph [0127], e.g., when the authentication fails, i.e., when the two message authentication codes do not coincide in the above example (step S12 NO), Nack message is returned to the device (step S15) and the subsequent access from the device 2 will not be transferred to the cellular phone network 6).

Therefore, taking teachings of Saito in combination of Malki and Inoue as a whole, it would have been obvious to one having ordinary skill in the art at the time of the invention by applicant by not performing a process relating to the change of the link connection of the mobile terminal which has failed in the authentication and a process relating to the authentication for the predetermined connection prohibition time after notification of authentication failure in a case where the authentication failure is notified as the authentication result with respect to the mobile terminal for advantages of providing a communication system in which a mobile terminal device belonging to some mobile carrier network can access a fixed communication network via a local network/gateway even when this mobile terminal device does not have a right or a qualification for accessing the fixed communication network via the local network/gateway that is given in advance (Inoue: paragraph [0014]).

Regarding claim 49 Saito in combination with Malki and Inoue discloses the radio communication management server according to claim 43 above, further comprising a registration control unit which controls to perform registration relating to the change of the link connection of the mobile terminal which has succeeded in the authentication only in a case where authentication success is notified as the authentication result with respect to the mobile

terminal (Inoue: paragraph [0126], e.g., When the authentication succeeds, i.e., when the two message authentication codes coincide in the above example (step S12 YES), Ack message is returned to the device 2 and the subsequent access from the device 2 will be transferred to the cellular phone network 6 (step S13) ).

Therefore, taking teachings of Saito in combination of Malki and Inoue as a whole, it would have been obvious to one having ordinary skill in the art at the time of the invention by applicant to perform registration relating to the change of the link connection of the mobile terminal which has succeeded in the authentication only in a case where authentication success is notified as the authentication result with respect to the mobile terminal for advantages of providing a communication system in which a mobile terminal device belonging to some mobile carrier network can access a fixed communication network via a local network/gateway even when this mobile terminal device does not have a right or a qualification for accessing the fixed communication network via the local network/gateway that is given in advance (Inoue: paragraph [0014]).

Regarding claim 50, Saito discloses a radio communication management server which manages link connection of a mobile terminal, comprising:

a receiving unit which receives information on authentication for accessing a desired network together with information for changing the link connection from the mobile terminal (Fig. 30, references S104 through S108; paragraphs [0010], [0015], [0019], [0022]- [0023], [0028], [0030], where Saito discusses the operation configuration for reporting a location change including authentication data each time a terminal moves between subnets, and achieves scalability an handoff by driving a network area into two layers using two different protocols),

a first transmitting unit which transmits, to the mobile terminal, the authentication result to the mobile terminal in a case where the authentication result is capable of being acquired within the time until acquiring the authentication result (paragraphs [0052], [0079], [0089], [0109], e.g., when the duplication check result for a current address of the mobile node is affirmative), and

a second transmitting unit which transmits, to the mobile terminal, information notifying the permission of the access to the desired network only for the predetermined tentative permission time (Fig. 6; paragraphs [0016], [0019], [0023]-[0024], [0269], [0355], e.g., the terminal device 302 determines whether authentication data stored in the binding update packet is valid or not, and if it is valid, then registers the care-of-address of the terminal 301).

Saito fails to specifically disclose setting a first time setting unit which, after receiving the information for changing the link connection, sets a time until acquiring an authentication result by an authentication process using the information on the authentication, and a second time setting unit which, after receiving the information for changing the link connection, sets a predetermined tentative permission time for which the mobile terminal tentatively permits an access to the desired network.

However, Inoue discloses setting a first time setting unit which, after receiving the information for changing the link connection, sets a time until acquiring an authentication result by an authentication process using the information on the authentication (paragraphs [0017], [0023], [0028], [0067], [0133], e.g., it is possible to enable the authenticated telephone network access by defining the authentication sequence between the home network device and the mobile

terminal device, and the access to the resource on the cellular phone network side is permitted only for the device that has successfully completed the authentication sequence).

Therefore, taking teachings of Saito in combination of Inoue as a whole, it would have been obvious to one having ordinary skill in the art at the time of the invention by applicant to set a time until acquiring the authentication result for advantages of providing a communication system in which a mobile terminal device belonging to some mobile carrier network can access a fixed communication network via a local network/gateway even when this mobile terminal device does not have a right or a qualification for accessing the fixed communication network via the local network/gateway that is given in advance (Inoue: paragraph [0014]).

Saito in combination with Inoue fails to disclose a second time setting unit which, after receiving the information for changing the link connection, sets a predetermined tentative permission time for which the mobile terminal tentatively permits an access to the desired network.

However, Malki discloses setting a predetermined tentative permission time for which the mobile terminal tentatively permits an access to the desired network (paragraph [0055], e.g., the lifetime of the bicasting should be set to no more than 10 seconds to limit the load imposed on the network by the bicasting).

Therefore, taking teachings of Saito in combination of Malki and Inoue as a whole, it would have been obvious to one having ordinary skill in the art at the time of the invention by applicant to set a predetermined permission time to permit the mobile terminal to access to the desired network while the authentication process is processing for advantages of improving communication processing for a mobile communication device.

Regarding claim 53, Saito in combination of Malki and Inoue discloses the radio communication management server according to claim 50 above, further comprising:

a prohibition time setting unit which sets a predetermined connection prohibition time with respect to the mobile terminal (Saito: paragraphs [0054], e.g., the gateway router set a lifetime of the routing cache for each mobile node in accordance with a routing update interval time); and

a prohibition control unit which controls to prevent a process relating to the mobile terminal which has failed in the authentication from being performed only for the predetermined connection prohibition time after notification of authentication failure in a case where the authentication failure is notified as the authentication result with respect to the mobile terminal (Inoue: paragraph [0127], e.g., when the authentication fails, i.e., when the two message authentication codes do not coincide in the above example (step S12 NO), Nack message is returned to the device (step S15) and the subsequent access from the device 2 will not be transferred to the cellular phone network 6).

Therefore, taking teachings of Saito in combination of Malki and Inoue as a whole, it would have been obvious to one having ordinary skill in the art at the time of the invention by applicant by not performing a process relating to the change of the link connection of the mobile terminal which has failed in the authentication and a process relating to the authentication for the predetermined connection prohibition time after notification of authentication failure in a case where the authentication failure is notified as the authentication result with respect to the mobile terminal for advantages of providing a communication system in which a mobile terminal device belonging to some mobile carrier network can access a fixed communication network via a local



network/gateway even when this mobile terminal device does not have a right or a qualification for accessing the fixed communication network via the local network/gateway that is given in advance (Inoue: paragraph [0014]).

Regarding claim 54, Saito in combination of Malki and Inoue discloses the radio communication management server according to claim 50 above, further comprising a registration control unit which controls to perform registration relating to the change of the link connection of the mobile terminal which has succeeded in the authentication only in a case where authentication success is notified as the authentication result with respect to the mobile terminal (Inoue: paragraph [0126], e.g., When the authentication succeeds, i.e., when the two message authentication codes coincide in the above example (step S12 YES), Ack message is returned to the device 2 and the subsequent access from the device 2 will be transferred to the cellular phone network 6 (step S13) ).

Therefore, taking teachings of Saito in combination of Malki and Inoue as a whole, it would have been obvious to one having ordinary skill in the art at the time of the invention by applicant to perform registration relating to the change of the link connection of the mobile terminal which has succeeded in the authentication only in a case where authentication success is notified as the authentication result with respect to the mobile terminal for advantages of providing a communication system in which a mobile terminal device belonging to some mobile carrier network can access a fixed communication network via a local network/gateway even when this mobile terminal device does not have a right or a qualification for accessing the fixed communication network via the local network/gateway that is given in advance (Inoue: paragraph [0014]).

4. Claim 9, 16, 46, and 51-52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Saito in combination with Malki and Inoue in view of Sawada et al. (hereinafter "Sawada"; US 2002/0016858; Cited in PTO-892 Part of Paper 20091008).

Regarding claims 9, 16, and 46, Saito in combination with Malki and Inoue discloses the radio communication management method and the radio communication management according to claims 1, 14, and 43 respectively above, wherein the server which manages the link connection sets the predetermined tentative permission time and for which the mobile terminal permits the access to the desired network (Malki: paragraph [0055], e.g., the lifetime of the bicasting should be set to no more than 10 seconds to limit the load imposed on the network by the bicasting), and transmits, to the mobile terminal, the information notifying the permission of the access to the desired network only for the predetermined permission time together with the information notifying that the change of the link connection of the mobile terminal has been confirmed in a case where the authentication result indicates authentication success (Saito: Fig. 6; paragraphs [0016], [0019], [0023]-[0024], [0269], [0355]).

Saito in combination with Malki and Inoue fails to specifically disclose setting a predetermined permission time which is longer than the predetermined tentative permission time.

However, Sawada discloses setting a predetermined permission time which is longer than the predetermined tentative permission time (paragraphs [0244], [0264], [0270]).

Therefore, taking teachings of Saito in combination of Malki, Inoue, and Sawada as a whole, it would have been obvious to one having ordinary skill in the art at the time of the invention by applicant to setting a predetermined permission time which is longer than the

predetermined tentative permission time for advantages of improving communication processing for a mobile communication device.

Regarding claim 51, Saito in combination with Malki and Inoue discloses the radio communication management server according to claim 50 above, further comprising:

a third transmitting unit which transmits, to the mobile terminal, the information notifying the permission of the access to the desired network only for the predetermined permission time in a case where the authentication result indicates authentication success (Saito: Fig. 6; paragraphs [0016], [0019], [0023]-[0024], [0269], [0355]).

Saito in combination with Malki and Inoue fails to specifically a third time setting unit which sets a predetermined permission time which is longer than the predetermined tentative permission time.

However, However, Sawada discloses setting a predetermined permission time which is longer than the predetermined tentative permission time (paragraphs [0244], [0264], [0270]).

Therefore, taking teachings of Saito in combination of Malki, Inoue, and Sawada as a whole, it would have been obvious to one having ordinary skill in the art at the time of the invention by applicant to setting a predetermined permission time which is longer than the predetermined tentative permission time for advantages of improving communication processing for a mobile communication device.

Regarding claim 52, Saito in combination of Malki, Inoue, and Sawada discloses the radio communication management server according to claim 51 above, further comprising:

a control unit which cuts the connection of the mobile terminal in a case where the predetermined tentative permission time or the predetermined permission time has elapsed

(Saito: paragraphs [0054], e.g., the gateway router set a lifetime of the routing cache for each mobile node in accordance with a routing update interval time), and does not perform a process relating to the mobile terminal which has failed in the authentication only for the predetermined connection prohibition time after notification of the authentication failure in a case where the authentication failure is notified as the authentication result with respect to the mobile terminal (Inoue: paragraph [0127], e.g., when the authentication fails, i.e., when the two message authentication codes do not coincide in the above example (step S12 NO), Nack message is returned to the device (step S15) and the subsequent access from the device 2 will not be transferred to the cellular phone network 6).

Therefore, taking teachings of Saito in combination of Malki, Inoue, and Sawada as a whole, it would have been obvious to one having ordinary skill in the art at the time of the invention by applicant by not performing a process relating to the change of the link connection of the mobile terminal which has failed in the authentication and a process relating to the authentication for the predetermined connection prohibition time after notification of authentication failure in a case where the authentication failure is notified as the authentication result with respect to the mobile terminal for advantages of providing a communication system in which a mobile terminal device belonging to some mobile carrier network can access a fixed communication network via a local network/gateway even when this mobile terminal device does not have a right or a qualification for accessing the fixed communication network via the local network/gateway that is given in advance (Inoue: paragraph [0014]).

***Conclusion***

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TIMOTHY PHAM whose telephone number is (571)270-7115. The examiner can normally be reached on Monday-Friday; 7:30AM-5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Vincent P. Harper can be reached on 571-272-7605. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ Timothy Pham/  
Examiner, Art Unit 2617

/VINCENT P. HARPER/  
Supervisory Patent Examiner, Art Unit  
2617